UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.
09/221,869	12/29/98	LINEHAN M	SE9-98-031(1

LM12/0927

STEVEN J MEYERS
IBM CORPORATION
INTELLECTUAL PROPERTY LAW BLGD 1
ROUTE 100 MP 1L1140
SOMERS NY 10589

EXAMINER	
HESS,R	
ART UNIT	**PAPER NUMBER**
2764	9

DATE MAILED: 09/27/00

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner of Patents and Trademarks

Office Action Summary	Application No.	Applicant(s)	
	09/221,869	LINEHAN, MARK	
	Examiner	Art Unit	
	Richard W. Hess	2764	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136 (a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).

Status

1)☒ Responsive to communication(s) filed on *09 August 2000* .

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-50* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☐ Claim(s) *1-50* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claims _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *29 December 1998* is/are objected to by the Examiner.

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. § 119

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d).

a)☐ All b)☐ Some * c)☐ None of the CERTIFIED copies of the priority documents have been:

1.☐ received.

2.☐ received in Application No. (Series Code / Serial Number) _____ .

3.☐ received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. & 119(e).

Attachment(s)

15) ☐ Notice of References Cited (PTO-892)
16) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
17) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
18) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
19) ☐ Notice of Informal Patent Application (PTO-152)
20) ☐ Other: .

DETAILED ACTION

1. Claims 1, 25–28, 33 and 34 have were amended and claims 46–50 were added by applicant's amendment filed 08/09/2000. Claims 1–50 have been examined.

Drawings

2. The corrected or substitute drawings were received on 08/09/2000. These drawings are acceptable for examining purposes only. Formal drawings will be required when the application is allowed.

Specification

3. Due to the changes effected by applicant's amendment filed 8/09/2000, the examiner has withdrawn the objection to the disclosure.

Claim Objections

4. Claim 50 is objected to because of the following informalities: Claim 50 reads like a dependent claim, but the applicant has failed to indicate upon which claim it is to depend. Appropriate correction is required.

For the purposes of the following art rejections, the examiner will assume that claim 50 depends upon claim 49.

Claim Rejections - 35 USC § 112

5. Due to the changes effected by applicant's amendment filed 8/09/2000, the examiner has withdrawn the 35 USC § 112, second paragraph rejections cited in the Office Action filed 5/10/2000.

Claim Rejections - 35 USC § 103

6. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

7. Claims 1–14 and 16–50 are rejected under 35 U.S.C. 103(a) as being unpatentable over Payne et al, US Patent 5,715,314, Elgamal, US Patent 5,671,279, Gifford, WO 95/16971, Anderson et al., "Description of Financial Agent Secured Transactions (FAST) Authentication," Financial Technology Consortium, Fourth Draft, December 2, 1998 and O'Mahony et al, Electronic Payment Systems, Artech House, Inc., Norwood, MA, 1997.

As per Claim 1, Payne et al teaches an electronic network commerce system comprising the steps of:

- Sending from a merchant's computer over an Internet network (column 4, lines 43–45) to a consumer's computer, a merchant message (column 5, lines 50–53). This merchant message includes a payment amount, an order description, a merchant digital signature (column 5, lines 29–46) and a timestamp (column 5, lines 39–40). Payne et al does not explicitly state that the merchant message contains a digital certificate from an acquiring bank as claimed by the applicant. Elgamal, however, expressly teaches that the message from the merchant to the customer in his electronic commerce system contains a digital certificate from the acquirer (column 9, lines 55–59). It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the teachings of Payne et al by including the certificate from the acquiring bank as taught by Elgamal to get the invention as

claimed by the applicant. The advantage would be to provide an important form of authentication in network commerce systems (Elgamal, column 4, lines 37–42)

- Payne et al also does not explicitly teach that the merchant message is a wallet initiation message and that this message starts a consumer's wallet program in the consumer's computer in response to the wallet initiation message. However, O'Mahony et al explicitly teaches that the merchant response from a consumer pay message initiates a wallet program in the consumer's computer (page 79, Section 4.6.3, paragraph 1, lines 1-5). It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the teachings of Payne et al with the wallet initiation message taught by O'Mahony et al for the advantage of making the purchasing steps as transparent as possible to the consumer by hiding the details of the payment steps and messages during a purchase (O'Mahony et al, page 78, Section 4.6.1, lines 1–4).
- Payne et al explicitly teaches sending from the consumer's computer, a message containing the consumer's identity and authentication information to a payment computer (including an issuer gateway for an issuing bank) (column 6, lines 30–43).
- Payne et al expressly teaches the issuer gateway verifies the merchant's signature to prove that the consumer is dealing with the actual merchant and validating, at the issuer gateway, the merchant's certificate and the acquirer's certificate to prove that the merchant and issuer share a common financial arrangement (column 5, lines 34–36, column 7, lines 24–27 and column 8, lines 3–5).

- Payne et al explicitly teaches that the issuer gateway verifies the consumer's account (column 6, lines 43–56) and ensures that funds and/or credit are available to support the payment amount (column 7, lines 14–15).
- Payne et al teaches that the payment computer (or issuer gateway) authorizes payment by sending over the Internet network an authorization token, an issuer's digital certificate, and a wallet initiation message (covered above). He also teaches that the authorization token includes the payment amount, order description, timestamp, a merchant identifier and a reference to the consumer's credit or debit card number (column 7, lines 14–30).
- Payne et al, however, does not explicitly state that the payment authorization message (token) contains a random nonce, but Gifford explicitly teaches issuing a payment order that includes a random nonce as claimed by the applicant (page 4, lines 21–28). It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the teachings of Payne et al by including a nonce in the payment authorization as taught by Gifford for the advantage of preventing a replay attack on the payment system (see page 48, Section 3.11 of O'Mahony et al).
- Payne et al explicitly teaches that once the merchant's computer receives the authorization token, the order description is fulfilled (column 7, line 49).

The amendment filed 08/09/2000 by the applicant added the limitation of forming a four party payment protocol for electronic sales. The four party payment protocol includes a consumer computer connected to a merchant and an issuing gateway. The four party payment protocol also includes a merchant computer connected to an

acquirer bank and the consumer computer via the Internet. According to O'Mahony et al, an issuer or issuing bank is a bank licensed by one of the major credit card companies (i.e. Visa or Master Card) that issues credit cards to customers. O'Mahony et al also states that merchants that wish to accept credit card payments must register with bank (not necessarily the consumer's issuer bank) which is called the acquiring bank or simply the acquirer (section 2.3 page 12–13). In fact, figure 2.3 on page 13 of O'Mahony et al shows the connection of the consumer (cardholder) to the issuer and the connection between the merchant and the acquiring bank as claimed by the applicant. The applicant also states that the connection is accomplished via a "gateway" connection. According to the Computer Dictionary (Third Edition, Microsoft Press, 1997, page 215) a "gateway" is "a device that connects networks using different communications protocols so that information can be passed from one to the other." Therefore, the applicant's addition of "forming a four party payment protocol for electronic sales, the four party payment protocol including a consumer's computer coupled to a merchant's computer and it an issuing bank computer via an issuer gateway, the merchant computer being further coupled to an acquirer bank computer" is just a description of connection topology used for credit card payments and is a well known and was commonly used at the time of the invention.

Adding the description of a well-known payment topology to the claim limitations already covered in the previous Office Action does not overcome the rejection of claim 1, so the rejection of this claim is maintained.

As per Claim 2, Payne et al expressly states that a start message is sent from consumer's computer over the internet network to the merchant's computer, to initiate the merchant's message (Figure 2A, number 32).

As per Claim 3, Payne et al teaches that the message received from the merchant in response to a buy message contains digital signature from the merchant (column 5, lines 42–43). Payne et al does not explicitly teach that the digital signature contains a nonce as claimed by the applicant. Elgamal, however, explicitly teaches that the message sent from the merchant to the consumer is also signed by the merchant (column 9, lines 56–60) and the signature contains a nonce (column 8, line16). It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the teachings of Payne et al with the inclusion of the nonce in the message sent from the merchant to the consumer as taught by Elgamal for the advantage of preventing a replay attack. The limitation that this message is a wallet initiation message was already covered in the rejection of Claim 1 above.

As per Claim 4, Payne et al explicitly teaches that the merchant's computer further performs the steps of receiving the authorization token (Figure 2H, number 92); verifying the issuer's signature, digital certificate, the payment amount and merchant identity in the authorization token (Figure 2H, number 94); verifying the freshness of the authorization token via the timestamp in the token (Figure 2H, number 98); and fulfilling said order description (Figure 2I, number 102). Payne et al does not explicitly state that a nonce in the authorization token is used to recognize duplicate tokens as claimed by the applicant. O'Mahony et al teaches that a nonce is used to recognize duplicate

tokens (page 48, Section 3.11 of O'Mahony et al). Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the teachings of Payne et al by using a nonce as taught by O'Mahony et al for the advantage of preventing a replay attack on the payment system.

As per Claim 5, Payne et al explicitly teaches the use of a userid and a password to identify the consumer (column 6, lines 43–44)

As per Claim 6, Payne et al teaches that the consumer interacts with a payment computer in his network sales system, but does not explicitly state that the payment computer is an ATM or a bank. Anderson et al teaches that FAST establishes a connection between the customer and the customer's bank by using a login and password (page 3, section 4.2). It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the teachings of Payne et al with the payment computer being the consumer's bank as taught by Anderson et al for the advantage of using an existing financial institution that is familiar to the consumer. Official Notice is also taken that both the concept and advantages of a bank using an ATM account debit card and password are well known and expected in the banking arts. It would have been obvious to use an ATM debit card number and PIN to identify a consumer because ATM accounts and PIN are a very common way for bank customers to interact with their bank and would avoid the confusion of creating multiple access accounts for the bank and the bank's customers.

Claims 7–13 describe a plurality of cryptographic ways to authenticate the consumer's identity in the claimed payment protocol. Official Notice is taken that both

the concept and advantages of the various ways to authenticate customers in a payment system as itemized in Claims 7–13 are well known and expected in the payment and cryptography arts. It would have been obvious to have provided these authentication methods because establishing the identity of a party in a payment system is an essential element in any payment system (see O'Mahony et al, pages 19 and 31).

As per Claim 14, Payne et al explicitly teaches that the issuer gateway sends the authorization token to the consumer and the consumer forwards the authorization token to the merchant (column 7, lines 31–33).

As per Claim 16, Payne et al explicitly teaches the use of an alias card number that is mapped at the issuing bank to a real card number thereby preventing use of the consumer's credit card number without the authorization token (Figure 7 and column 6, lines 15–29).

As per Claim 17, Payne et al does not expressly state the use of an authorization number in the message sent back to the merchant. Gifford teaches the use of an authorization number allocated uniquely by the issuer gateway for each authorization (page 6, lines 20–23). Gifford also teaches that the issuing bank (payment computer) maintains a database mapping of authorization numbers to card numbers, so that when the issuing bank receives the capture message, it uses the database mapping to determine the consumer's card number (page 15, lines 16–27 and Figure 13). It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the teachings of Payne et al with the authorization number system taught by

Gifford for the advantage of providing added security for users who are reluctant to use their actual credit card numbers over the payment network.

As per Claim 18, Payne et al does not expressly state the use of an authorization token containing a dummy number for use in routing payment to an appropriate one of a plurality of issuing banks, such that the dummy card number is shared among all card holders of a particular issuing bank. Official Notice is taken that both the concept and advantages of using a dummy number (such as a bank identification number (BIN)) are well known and expected in the credit card and banking arts. It would have been obvious to use such a number because it would increase the efficiency of transmitting the electronic payment instructions through existing clearing house systems.

As per Claims 19–23, Official Notice is taken that both the concept and advantages of using various authorization certificate hierarchies are well known and expected in the electronic commerce arts. It would have been obvious to include he various certificate arrangements cited in Claims 19–23 in order to make sure that all parties in the payment protocol are trusted and are who the claim to be in any transaction.

As per Claim 24, Payne et al does not explicitly teach the payment protocol for the case of a split shipment as claimed by the applicant. Elgamal specifically covers the payment protocol for split shipments as claimed by the applicant (column 13, line 64 through column 14, line 7). It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the teachings of Payne et al with the split

shipment payment protocol taught by Elgamal for the advantage of handling partial shipments.

As per Claim 25, Payne et al teaches that his sales system can buy a plurality of products and add these products to a shopping cart (column 7, line 55 through column 8, line 2), but he does not explicitly disclose including "Japanese Payment Options" (installment payments) as claimed by the applicant. Elgamal explicitly teaches that his payment protocol covers periodic payments (column 13, lines 53–63). It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the teachings of Payne et al with the periodic payment capability taught by Elgamal for the advantage of making car payment or other periodic payments.

Claims 26, 27 and 28 are apparatus and program code claims that contain the same limitations already covered in the rejection of Claim 1, so the same rejections apply to these Claims.

Claims 29, 30 and 31 contain the same limitations already covered in the rejections of Claims 2, 3 and 4 respectively, so the same rejections apply to the rejections of Claims 29–31.

As per Claim 32, Payne et al teaches using an account number associated with the payment computer, but does not explicitly teach using the consumer's credit or debit card number as claimed by the applicant. Elgamal, however, explicitly teaches including the consumer's credit or debit card account number in the payment instruction message (column 10, lines 1–33). It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the teachings of Payne et al by

referring to the actual consumer's credit or debit account number as taught by Elgamal for the advantage of being able to directly access the consumer's account without having to go through a intermediary account translation file.

Claim 33 contains the same method steps already covered in the rejection of Claim 1, so the same rejections apply to the rejection of this Claim. The applicant, however, includes one additional limitation concerning the use of a URL to identify the network location of the acquiring bank contacted via an Internet network as part of the payment protocol. Official Notice is taken that both the concept and advantages of using a URL to locate a particular location on the Internet are well known and expected in the Internet and network communication arts, because the URL address structure has been used on the Internet since its inception.

Claim 34 contains the same limitations already covered in the rejections of Claims 1, 7-10, 18 and 23–26, so the same rejections apply to the rejection of this Claim.

Claim 35 contains the same limitation already covered in the rejections of Claims 1 and 19, so the same rejections apply to the rejection of this Claim.

Claim 36, contains the same limitation already covered in the rejections of Claims 1 and 19–23, so the same rejections apply to the rejection of this Claim.

Claims 37–39 contain the same limitations already covered in the rejections of Claims 32, 3 and 4 so the same rejections apply to the rejections of Claims 37–39.

As per Claims 40–42, Payne et al teaches the sales process but does not cover the steps necessary for a capture process in a payment protocol. Elgamal, however,

covers the capture process steps as claimed by the applicant in Claims 40–42 (column 11, line 43 through column 12, line 63). It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the teachings of Payne et al with the capture process taught by Elgamal for the advantage of actually settling the account between buyers and merchants as is common practice in almost any payment protocol.

As per Claim 43, Payne et al explicitly teaches hashing the order information before it is sent to the merchant and also teaches that the hashing function is known by the payment computer and the merchant (column 7, line 65 through column 8, line 2). Official Notice is taken that both the concept and advantages of the merchant validating that the authorization token refers to the same order description by comparing the hash of the order description in the authorization token against a locally-computed hash of the same order description are well known and expected in the cryptographic arts. The very nature of hashing is to assure that the hashed data has not been altered by comparing the sent hash value to the hash value obtained by the recipient of the data.

Claim 44 contains the same limitations already covered in the rejection of Claim 32, so the same rejection applies to the rejection of this Claim.

As per Claim 45, Official Notice is taken that both the concept and advantages of using higher-level security protocols such as SSL are well known and expected in the encryption arts. It would have been obvious to use higher-level security protocols such as SSL because it would allow the payment protocols to be used open public networks

such as the Internet. In fact SSL was developed for secure communication on the Internet (O'Mahony et al, page 72, second paragraph).

As per Claims 46–50, these claims contain the same limitations already covered in the rejection of claim 1, so the same rejection applies to Claims 46–50.

8. Claim 15 is rejected under 35 U.S.C. 103(a) as being unpatentable over Payne et al, Elgamal, Gifford, Anderson et al and O'Mahony et al, as applied to Claim 1 above, and further in view of Ogram, US Patent No. 5,822,737.

As per Claim 15, Payne et al teaches that the payment computer sends a redirect message to the buyer computer and this message is forwarded to the merchant computer (column 7, lines 31–33). Payne et al goes on to teach that a portion of the information contained in the message forwarded to the merchant is encrypted so that only the payment computer and the merchant can view the contents of the message (column 7, line 24–30). Since the encrypted portion of the message is only viewable by the payment computer and the merchant, this portion of the message would inherently be sent directly to the merchant as claimed by the applicant. Payne et al, however, does not explicitly show a direct connection from the payment computer to the merchant as claimed by the applicant. Ogram explicitly shows the direct connection between the payment computer and the merchant (Figure 2D). It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the teachings of Payne et al with the with the direct connection taught by Ogram for the advantage of making sure the message went through when the customer's computer was

disconnected and the payment computer was ready to send information intended specifically for the merchant.

Response to Arguments

9. Applicant's arguments filed 08/09/2000 have been fully considered but they are not persuasive for the following reasons:

On pages 13–20, the applicant offers his summary of the references cited in the Office Action filed 5/10/2000. The examiner has reviewed the applicant's synopsis of the cited references, but does not agree with the applicant's summarizing statement in the last paragraph on page 20. The examiner maintains that the obvious combination of the cited references does indeed teach and show all the elements in the invention claimed by the applicant. The examiner also maintains that the rejections put forth above and in the previous Office Action present a *prima facie* case for rejecting the applicant's application for patent protection.

In general, the arguments presented by the applicant from the bottom of page 21 through the middle of page 27 are that none of the cited references individually contain all the limitations contained in claims 1–45. The applicant then jumps to the conclusion that the references "taken alone or in combination" do not disclose the features of the claimed invention. The applicant also does not present any arguments challenging the examiner's logic and/or motivation for stating that a person of ordinary skill in the art at the time of the invention would make the obvious combination of the cited references to obtain the applicant's invention. Since no challenges were made about the combined teachings of the cited references, the examiner must assume that the applicant's sole

argument is that since the individual reference do not individually show all the features of the claimed invention then their combination also does not show the features of the claimed invention. The courts, however, have held that "one cannot show non-obviousness by **attacking references individually** where rejections are based on combinations of references" (In re Keller, Terry, and Davies, 208 USPQ 871 (CCPA 1981) and "non-obviousness cannot be established by attacking references individually where the rejection is based upon the teachings of a combination of references' (In re Merck & Co., Inc., 231 USPQ 375 (CA FC 1986).

Therefore the examiner's rejection of claims 1–45 are maintained.

The rejection on the new claims 46–50 was presented above.

Conclusion

10. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Richard W. Hess whose telephone number is (703) 308-6287. The examiner can normally be reached on M-F (7:00-4:30) First Friday Off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James P. Trammell can be reached on (703) 305-9768. The fax phone numbers for the organization where this application or proceeding is assigned are (703) 308-9051 for regular communications and (703) 308-5357 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

Richard W. Hess
September 25, 2000

James P. Trammell
Supervisory Patent Examiner
Technology Center 2700